UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,946	03/31/2000	Carl M. Ellison	042390.P8104	3228

7590 03/08/2006

Thinh V Nguyen
Blakely Sokoloff Taylor & Zafman LLp
12400 Wilshsire Boulevard
7th Floor
California, CA 90025

EXAMINER	
HENEGHAN, MATTHEW E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/540,946	ELLISON ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-21,23-33,35-45 and 47-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-21,23-33,35-45 and 47-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claim 25; added claims 49-52; and cancelled claims 10, 22, 34, and 46. Claims 1-9, 11-21, 23-33, 35-45, and 47-52 have been examined.

Specification

2. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Nothing in Applicant's specification provides support for the term "tangible computer readable program code" as presented in claim 25.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 25-33, 35, 36, and 51 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement and as failing to comply with the enablement requirement. The claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in

the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention, and which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

In claim 25, the term "tangible computer readable program code" was not used in the original disclosure; moreover, it is unclear how one skilled in the art would create computer readable program code that is tangible.

Claims 26-33, 35, 36, and 51 depend from rejected claim 25, and include all the limitations of that claim, thereby rendering those dependent claims as failing to comply with the written description requirement and as failing to comply with the enablement requirement.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 25-33, 35, 36, and 51 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Since no basis is given that would allow one skilled in the art to differentiate between computer readable program code that is tangible, as opposed to that that is intangible, claim 25 is indefinite.

Claims 26-33, 35, 36, and 51 depend from rejected claim 25, and include all the limitations of that claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-9, 11, 12, and 49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 teaches solely to a set of software modules, with constitutes functional descriptive material that is not tangibly embodied.

Claims 2-9, 11, 12, and 49 depend from rejected claim 1, and include all the limitations of that claim, thereby rendering those dependent claims non-statutory.

Claim Rejections - 35 USC §103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-9, 11-21, 23-33, 35-45, 47, and 48 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 5,421,006 to Jablon et al. in view of U.S. Patent No. 6,327,652 to England et al.

As per claims 1, 2, 4, 7, 13, 14, 16, 19, 25, 26, 28, 31, 37, 38, 40, and 43, the system integrity scheme disclosed by Jablon includes the use of keys (using encryption) for each program level, including parts of the operating system, for protecting (a usage protector) a subset of the operating system's environment (see column 16, lines 36-44 and column 19, lines 28-44). The subset of the operating system that is loaded to the lowest level constitutes an OS nub. Jablon's environment is directed towards security and thus constitutes a secure platform (see column 1, lines 10-16).

Though each level's private key is employ the level's MDC (which is unique) and the public key of a trusted authority (the BK0) and stored and retrieved as a signature, the MDC does not constitute a key; therefore Jablon does not disclose either a unique key for each program portion or a key generator.

England discloses a key generator (see column 7, lines 45-62) that creates unique keys for each targeted program (see column 17, lines 1-18), and further suggests that it is necessary to keep keys secret from other OS's or other system level software (see column 16, lines 50-55).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Jablon by using a key generator to generate unique keys for each program, such as the OS nub, as disclosed by England, as it is necessary to keep keys secret from other OS's or other system level software.

Though Jablon's exemplary embodiment employs a ringless operating system, DOS, the invention disclosed by Jablon would clearly work with a ringed system; moreover, Jablon discloses that the invention may be used with other operating systems (see column 10, lines 23-24) and specifically notes a ringed operating system, UNIX, that would benefit from the Jablon's invention (see column 3, lines 12-23). The claimed invention is therefore anticipated by Jablon.

Alternatively, it is also noted that Jablon only discloses a ringless embodiment (using DOS), though the invention may be used with other operating systems (see column 10, lines 23-24).

Jablon notes that UNIX, despite its ringed architecture, needs additional protection, as preventing root access is a well-known security problem of the system (see column 3, lines 12-23).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement the invention disclosed by Jablon in a ringed operating system, such as UNIX, as preventing root access is a well-known security problem of the system.

As per claims 3, 15, 27, and 39, Jablon discloses that the MDC may be a hash value (see column 5, lines 44-47).

As per claims 5, 17, 29, and 41, a second hash is computed and compared to the original for verification (see column 19, lines 39-44).

As per claims 6, 18, 30, and 42, a layer of the OS, the login file may be stored encrypted, and decrypted for verification (see column 22, lines 47-56).

As per claims 8, 20, 32, and 44, a list of programs (the manifest) may be kept, with all the above-mentioned integrity information (see column 17, line 48 to column 18, line 24).

As per claims 9, 21, 33, and 45, the invention uses a latch to protect the system from untrusted software (isolated execution) (see abstract).

Regarding claims 11, 23, 35, and 47, the list of programs encompasses all of the programs running at the level immediately below a program. The level immediately below the operating system (DOS) is defined by the registry, and there therefore exists such a list.

As per claim 12, 24, 36, and 48, BK0 may also come from the boot record, which is at the highest level, which may include a random element calculated during the bootup sequence (see column 15, lines 1-9).

7. Claims 49-52 are rejected under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 5,421,006 to Jablon et al. in view of U.S. Patent No. 6,327,652 to England et al. as applied to claims 1, 13, 25, and 37 and further in view of U.S. Patent No. 4,787,031 to Karger et al.

Jablon specifically cites the multi-ringed architecture disclosed by Karger (see Jablon, column 3, lines 9-11 and Karger, entire document), and Jablon suggests that, despite the architectural strength of such systems, the integrity of trusted software cannot always be guaranteed (see Jablon, column 3, lines 12-14). Karger discloses a four-ring architecture (see Karger, figure 2A).

Therefore it would been obvious to one of ordinary skill in the art at the time the invention was made to utilize the invention of Jablon and England in the multi-ring architecture of Karger, as the integrity of trusted software cannot always be guaranteed.

Terminal Disclaimer

8. The terminal disclaimer filed on 14 December 2005 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on Patent Application No. 09/668,610 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Double Patenting

9. In view of the filing of a terminal disclaimer, all previous rejections over double patenting are withdrawn.

Response to Arguments

10. Applicant's arguments filed 14 December 2005 regarding the rejections of claims 1-9, 11, and 12 under 35 U.S.C. 101 of claims 1-9, 11, and 12 have been fully considered but they are not persuasive. Though Applicant's specification states that the usage protector may be implemented in software or hardware, the only embodiment

that is actually described in the disclosure is clearly implemented in software; moreover, the claim as presented, at the very least, encompasses an embodiment that is entirely composed of non-statutory subject matter (the software implementation). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In Applicant's reference to figures 3A-3C, it is noted that the storage and the hardware-implemented comparator (comparators may also be implemented in software) are not specified in the claims. The rejections are therefore proper.

11. Applicant's arguments with respect the rejections under 35 U.S.C. 101 with respect to claims 25-33, 35, and 36 as amended have been considered but are moot in view of the new grounds of rejection under 35 U.S.C. 112, above.

12. Applicant's arguments with respect to claims 1-9, 11-21, 23-33, 35-45, 47, and 48 have been considered but are moot in view of the new ground(s) of rejection.

Regarding Applicant's first argument, as was noted in the previous office action, that Jablon does not teach a ring hierarchy, a ringed architecture, as depicted in Figure 1A of the instant application, with respect to a computer operating is one in which programs and data are encapsulated in one of a plurality of levels, where programs in any one level are disabled from accessing the memory contained within a lower-numbered ring; the programs and data of the lower ring may only be accessed via predefined system calls.

The exemplary embodiment disclosed by Jablon is implemented in PC DOS, an operating system that is implemented, for example, on an Intel 8088 microprocessor. Since the 8088 on a PC has an architecture such that any program on the computer may access any memory location without restriction, it is impossible to design an invention for this platform that completely restricts memory access to any particular region; because of this, a ringed architecture, which serves to regulate communication among various regions, cannot be implemented. Since there is no means in the processor to restrict access, the greatest benefit of Jablon's invention, which uses encryption to regulate access between different designated regions, would be realized in such an environment. It is for this reason that Jablon chose an operating system native to a PC for the exemplary embodiment. As has been noted in the Office actions, Jablon also specifically notes that this invention is applicable to other operating systems (see Jablon, column 10, lines 19-24, as well as column 1, lines 34-42).

Nonetheless, since the *raison d'être* for a ringed architecture is the prohibition of computer accesses to more secure areas, one skilled in the art would see that any mechanism that is operable among the hierarchical rings in a ringed architecture and offers greater security in inter-ring accessing would also be advantageous. Jablon noted as much in discussing UNIX (see Jablon, column 3, lines 12-23), specifically noting that, despite UNIX's ringed architecture, unauthorized accesses remain a well-known problem of the system.

Though it is stated that Jablon's invention is only intended for systems lacking a "strong protection architecture," as Applicant has noted, it must be concluded from

Jablon's observations pertaining to UNIX's security flaws that Jablon does not consider UNIX's protection architecture to be "strong."

It is therefore the case that, although the invention disclosed by Jablon is described in terms of a DOS environment, Jablon also intended to apply the invention to a ringed operating system such as UNIX, and Applicant's claims are thus obvious in view of the added benefits to a ringed architecture, such as UNIX, that Jablon has explicitly recognized.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (571) 272-3859.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

February 27, 2006

HOSUK SONG
PRIMARY EXAMINER